

MUTUALLY UNBIASED BASES FOR QUANTUM STATES DEFINED OVER p -ADIC NUMBERS

WIM VAN DAM AND ALEXANDER RUSSELL

ABSTRACT. We describe sets of mutually unbiased bases (MUBs) for quantum states defined over the p -adic numbers \mathbb{Q}_p , i.e. the states that can be described as elements of the (rigged) Hilbert space $L^2(\mathbb{Q}_p)$. We find that for every prime $p > 2$ there are at least $p + 1$ MUBs, which is in contrast with the situation for quantum states defined over the real line \mathbb{R} for which only 3 MUBs are known. We comment on the possible reason for the difference regarding MUBs between these two infinite dimensional Hilbert spaces.

1. MUTUALLY UNBIASED BASES

Let $V = \{v_1, \dots, v_d\}$ and $W = \{w_1, \dots, w_d\}$ be two orthonormal bases for the d -dimensional Hilbert space $L^2(\mathbb{Z}/d\mathbb{Z}) \simeq \mathbb{C}^d$. We say that V and W are *mutually unbiased bases* (MUBs) if and only if all vectors of V are a uniform, unbiased superposition in terms of the W vectors, and vice versa. It is straightforward to show that this is equivalent with the requirement $|\langle v_i | w_j \rangle| = 1/\sqrt{d}$ for all $i, j \in \{1, \dots, d\}$. A set $\{V_1, \dots, V_N\}$ of bases is mutually unbiased if and only if each proper pair V_k, V_ℓ (with $k \neq \ell$) of bases is mutually unbiased. As an example, for the qubit $d = 2$ case we have a set of three MUBs: $V_1 = \{|0\rangle, |1\rangle\}$, $V_2 = \{(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$, and $V_3 = \{(|0\rangle + i|1\rangle)/\sqrt{2}, (|0\rangle - i|1\rangle)/\sqrt{2}\}$. Mutually unbiased bases play an important role in the problem of optimal quantum state estimation [15], quantum cryptography [5] and the construction of discrete Wigner functions [6].

A central question in the theory of finite dimensional MUBs is what the maximal cardinality $N(\mathbb{C}^d)$ is of a set of MUBs for a given dimension d . It can be shown that $N(\mathbb{C}^d) \leq d + 1$ and we also know that if d is a power of a prime, p^r , then this bound can be achieved: $N(\mathbb{C}^{p^r}) = p^r + 1$. (Below we will give an explicit construction of $p^r + 1$ MUBs in \mathbb{C}^{p^r} .) For dimensions that are not a prime power, the same question is wide open. For $d = 6$ we know that there are 3 MUBs and several extensive numerical computations suggest that this is largest possible number of MUBs in \mathbb{C}^6 . However, despite significant efforts on this $N(\mathbb{C}^6) = 3?$ question, we still do not have a rigorous proof that excludes the possibility that $N(\mathbb{C}^6) = 7$. More generally for $d = p_1^{r_1} \cdots p_k^{r_k}$ it is known that $N(\mathbb{C}^d) \geq 1 + \min_i p_i^{r_i}$ (Lemma 3 in [8]), but to strengthen this bound has proven to be difficult, although not impossible for certain very specific cases [14].

1.1. The “ $(ax^2 + bx)$ construction” of $(p^r + 1)$ MUBs in dimension p^r .

It is notable that, although the question of MUBs is a purely geometric one, the constructions often involve nontrivial results in number theory. The following construction of a maximal set of $p^r + 1$ mutually unbiased bases in \mathbb{C}^{p^r} is a quintessential example of this [1, 8].

Example 1. Let p be a prime and $r \in \mathbb{Z}^+$ a positive exponent. Using the finite field \mathbb{F}_{p^r} and its trace operation $\text{tr} : \mathbb{F}_{p^r} \rightarrow \mathbb{F}_p$ with $\text{tr} : x \mapsto x + x^p + x^{p^2} + \cdots + x^{p^{r-1}}$, we define the following set of p^r bases V_a indexed by $a \in \mathbb{F}_{p^r}$:

$$(1) \quad V_a := \{|v(a, b)\rangle : b \in \mathbb{F}_{p^r}\} \text{ with } |v(a, b)\rangle := \frac{1}{\sqrt{p^r}} \sum_{x \in \mathbb{F}_{p^r}} e^{2\pi i \text{tr}(ax^2 + bx)/p} |x\rangle.$$

Combined with the computational basis $V_\infty := \{|b\rangle : b \in \mathbb{F}_{p^r}\}$, the set of $p^r + 1$ bases $\{V_a : a \in \mathbb{F}_{p^r} \cup \{\infty\}\}$ is mutually unbiased. This fact can be proven using standard results on quadratic Gauss sums [3]. That the V_∞ vectors are mutually unbiased to the V_a vectors follows trivially from the fact that all amplitudes of all $v(a, b)$ have norm $1/\sqrt{p^r}$. To prove that the V_a bases are mutually unbiased one should first observe that

$$(2) \quad \langle v(a', b') | v(a, b) \rangle = \frac{1}{p^r} \sum_{x \in \mathbb{F}_{p^r}} e^{2\pi i ((a-a')x^2 + (b-b')x)}.$$

The mutually unbiasedness is then proven by the following result on quadratic Gauss sums over finite fields

$$(3) \quad \left| \sum_{x \in \mathbb{F}_{p^r}} e^{2\pi i \text{tr}(\alpha x^2 + \beta x)} \right| = \begin{cases} \sqrt{p^r} & \text{if } \alpha \neq 0 \\ 0 & \text{if } \alpha = 0 \text{ and } \beta \neq 0 \\ p^r & \text{if } \alpha = 0 \text{ and } \beta = 0. \end{cases}$$

Gauss sums $\sum_s e^{2\pi i (ax^2 + bx)/d}$ over a ring $\mathbb{Z}/d\mathbb{Z}$ behave ‘less nicely’ when d is not prime, which prevents the above $(ax^2 + bx)$ construction to work for arbitrary dimensions d . Nevertheless, we will use this construction to find MUBs for infinite dimensional Hilbert spaces.

1.2. MUBs for infinite dimensional Hilbert spaces? It is a non-trivial question to ask if one can define mutually unbiased bases for infinity dimensional Hilbert space and, if this is indeed possible, how many MUBs exist in such spaces. Weigert and Wilkinson[13] did exactly this for quantum variables defined over the real line and they found only 3 MUBs in this Hilbert space $L^2(\mathbb{R})$. The three bases they found were the (generalized) eigenvectors of operators that are a combination of the position operator \hat{q} and the momentum operator \hat{p} ; the three operators they used are \hat{q} , $\cos(\frac{2\pi}{3})\hat{q} + \sin(\frac{2\pi}{3})\hat{p}$ and $\cos(\frac{2\pi}{3})\hat{q} - \sin(\frac{2\pi}{3})\hat{p}$.

1.3. Our Result. Partly in response to the $N(L^2(\mathbb{R})) \geq 3$ result of Weigert and Wilkinson, Blume-Kohout wondered ‘Is ∞ prime? or possibly a multiple of 2?’ [4]. The idea being that if the infinite dimension of $L^2(\mathbb{R})$ is ‘prime’, we would expect $N(L^2(\mathbb{R})) = \infty + 1$, whereas if the dimension is even, then maybe indeed $N(L^2(\mathbb{R})) = 3$, just as we seem to have $N(\mathbb{C}^6) = 3$. Our result here shows that the answer to Blume-Kohout’s question likely depends on properties of the Hilbert space that go beyond the fact that its dimensionality is infinite. We do this by considering quantum states that are defined over the p -adic numbers \mathbb{Q}_p , i.e. we look at MUBs in the infinite dimensional Hilbert space $L^2(\mathbb{Q}_p)$. Using the $(ax^2 + bx)$ construction of the previous section and the theory of quadratic Gauss integrals over \mathbb{Q}_p , we show that for each prime $p > 2$ one has the lower bound $N(L^2(\mathbb{Q}_p)) \geq p + 1$.

For functions in $L^2(\mathbb{Q}_p)$ we have a well-defined notion of continuity and \mathbb{Q}_p is an infinite, locally compact Abelian group, just like \mathbb{R} . In this sense, \mathbb{Q}_p defines a continuous variable that is different from \mathbb{R} and one can study the idea of “ p -adic

quantum mechanics”, which has been done already by various authors [9, 11, 12]. In the next section we will provide the necessary definitions to work with the Hilbert space $L^2(\mathbb{Q}_p)$. After that, in Section 3, we describe a construction of $p + 1$ MUBs in this space, and prove their mutually unbiasedness. In the last two sections we address the question why MUBs for real valued variables seem to behave differently from those defined over \mathbb{Q}_p .

2. p -ADIC QUANTUM MECHANICS

2.1. p -adic numbers. An excellent introduction to p -adic numbers is provided by Gouvêa [7]; here we will mostly recite the necessary basic definitions. Consider the possible norms on the field of rational numbers \mathbb{Q} . Besides the standard \mathbb{R} norm, we also have the p -adic norm $|\cdot|_p$ for each prime integer p as a possibility, which is defined as follows. For $x \in \mathbb{Q} \setminus \{0\}$, write $x = p^v(a/b)$ where v, a, b are all integers and p does not divide a or b . The $v \in \mathbb{Z}$ is called the *valuation* $v_p(x)$ of x ; additionally we define $v_p(0) := +\infty$. The p -adic norm is defined by $|x|_p := p^{-v_p(x)}$. The completion of \mathbb{Q} under this norm gives rise to the p -adic numbers \mathbb{Q}_p . The p -adic integers \mathbb{Z}_p in \mathbb{Q}_p are those elements $z \in \mathbb{Q}_p$ with $|z|_p \leq 1$, i.e. those with $v_p(z) \geq 0$. (The ring of p -adic integers \mathbb{Z}_p should not be confused with the field $\mathbb{Z}/p\mathbb{Z}$ of integers modulo p , although some authors denote this field also by \mathbb{Z}_p .) Note that with this norm, the limit $\lim_{k \rightarrow +\infty} p^k$ converges to 0, and hence $1 + \lim_{k \rightarrow +\infty} (p^k - 1) = 0$, showing that $-1 = p - 1 + \sum_{j=2}^{+\infty} p^j$ in \mathbb{Q}_p . The observation supports the following notation.

Each nonzero p -adic number $z \in \mathbb{Q}_p$ can be described by the formal power series

$$(4) \quad z = \sum_{j=v_p(z)}^{+\infty} z_j p^j \text{ with } z_j \in \{0, \dots, p-1\} \text{ for all } j \geq v_p(z) \text{ and } z_{v_p(z)} \neq 0.$$

The sets \mathbb{Z}_p and \mathbb{Q}_p are both uncountable; \mathbb{Z}_p is compact, while \mathbb{Q}_p is only locally compact. Just as the field \mathbb{Q}_p shares many properties with \mathbb{R} , the ring $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ has several similarities with $\mathbb{R}/\mathbb{Z} \simeq \{x \in \mathbb{R} : |x| < 1\}$.

For each $\mathbb{Q}_p \ni z = \sum_{j=v}^{\infty} z_j p^j$ its *fractional part* is defined by $\{z\} := \sum_{j=v}^{-1} z_j p^j$. For all $z \in \mathbb{Q}_p$ we have that $\{z\}$ is a rational number from the set $\{m/p^n : n \in \mathbb{Z}^+, m \in \{0, \dots, p^n - 1\}\}$; one can also view this value as $\{z\} = z \bmod \mathbb{Z}_p$. We define the function $e : \mathbb{Q}_p \rightarrow \mathbb{C}$ by $e(x) = \exp(2\pi i \{x\})$ such that $|e(x)| = 1$ for all x . Note that, while $\{x + y\}$ does not always equal $\{x\} + \{y\}$, it does hold that $e(x + y) = e(x)e(y)$, making e an additive character of \mathbb{Q}_p that is trivial on \mathbb{Z}_p . For each $\alpha \in \mathbb{Q}_p$ the $\mathbb{Q}_p \rightarrow \mathbb{C}$ function $x \mapsto e(\alpha x)$ is an additive character on \mathbb{Q}_p and all characters can be expressed this way, hence \mathbb{Q}_p is its own Pontryagin dual [10]. For characters over \mathbb{Z}_p we have that $e(\alpha x) = e((\alpha + 1)x)$ for all $x \in \mathbb{Z}_p$, which shows that only the fractional part of α matters in this context. Indeed one can show that the dual of \mathbb{Z}_p is equivalent to the group $\mathbb{Q}_p/\mathbb{Z}_p$.

2.2. Measures on \mathbb{Q}_p , quantum states over \mathbb{Q}_p , and $L^2(\mathbb{Q}_p)$. The standard, normalized Haar measure μ on \mathbb{Q}_p is given by $\mu(p^j \mathbb{Z}_p) = p^{-j}$ such that $\mu(\mathbb{Z}_p) = 1$ and, for $z \in \mathbb{Q}_p$, we have $\mu(z + p^j \mathbb{Z}_p) = p^{-j}$ where $z + S = \{z + x : x \in S\}$. Notice that $\mu(\mathbb{Q}_p) = +\infty$. From now on, an integral $\int_{x \in \mathbb{Q}_p} dx$ is understood to be taken with respect to this measure. The Hilbert space $L^2(\mathbb{Q}_p)$ has as its elements

$$(5) \quad L^2(\mathbb{Q}_p) := \{\psi : \mathbb{Q}_p \rightarrow \mathbb{C} : \|\psi\| < \infty\}$$

with the ℓ_2 -norm defined by

$$(6) \quad \|\psi\| := \sqrt{\int_{x \in \mathbb{Q}_p} \psi(x) \psi^*(x) dx}.$$

A function/quantum state ψ is *normalized* when $\|\psi\| = 1$.

2.3. Fourier transforms in $L^2(\mathbb{Q}_p)$. For a function $\psi \in L^2(\mathbb{Q}_p)$, its *Fourier transform* $\hat{\psi} : \mathbb{Q}_p \rightarrow \mathbb{C}$ is defined by

$$(7) \quad \hat{\psi}(y) = \int_{x \in \mathbb{Q}_p} \psi(x) e(xy) dy \text{ for all } y \in \mathbb{Q}_p.$$

Example 2. Fix $r \in \mathbb{Z}$ and $z \in \mathbb{Q}_p$. Define the function $\psi \in L^2(\mathbb{Q}_p)$ by

$$(8) \quad \psi(x) = \begin{cases} p^{r/2} & \text{if } x \in z + p^r \mathbb{Z}_p \\ 0 & \text{otherwise.} \end{cases}$$

Notice that ψ is normalized with $\|\psi\| = 1$ and that with the p -adic distance between the elements of \mathbb{Q}_p this indicator function is continuous. The Fourier transform of ψ is described by

$$(9) \quad \hat{\psi}(y) = \begin{cases} e(yz) \cdot p^{-r/2} & \text{if } y \in p^{-r} \mathbb{Z}_p \\ 0 & \text{otherwise.} \end{cases}$$

As the Fourier transform is a isometry from $L^2(\mathbb{Q}_p)$ to itself (under the natural inner product given by Haar measure), such ψ are the natural \mathbb{Q}_p -equivalents of the Gaussian distribution over \mathbb{R} with r acting as the scale.

3. $(p+1)$ MUTUALLY UNBIASED BASES IN $L^2(\mathbb{Q}_p)$

Just as in the $L^2(\mathbb{R})$ case of Weigert and Wilkinson [13], our MUBs are ‘generalized’ eigenstates, meaning that they are not properly normalized. To deal with this issue we will use the standard technique of describing them as a limit of functions that *are* elements of $L^2(\mathbb{Q}_p)$. The limit that we will rely upon is $\lim_{r \rightarrow +\infty} p^{-r} \mathbb{Z}_p = \mathbb{Q}_p$ (as sets). (All of this can be made more rigorous by casting it in the framework of ‘rigged’ Hilbert spaces [2].) We allow ourselves the slight abuse of notation where

$$(10) \quad L_2(\mathbb{Q}_p) \ni |\psi\rangle = \int_{x \in \mathbb{Q}_p} \psi(x) |x\rangle dx \text{ stands for } \psi : \mathbb{Q}_p \rightarrow \mathbb{C} \text{ with } \psi : x \mapsto \psi(x).$$

For each $r \in \mathbb{Z}$ we define the following sets $V_a^{(r)} \subseteq L^2(\mathbb{Q}_p)$ indexed by $a \in \mathbb{Q}_p$:

$$(11) \quad V_a^{(r)} := \{|v(a, b; r)\rangle : b \in \mathbb{Q}_p\} \text{ with } |v(a, b; r)\rangle := \int_{x \in p^{-r} \mathbb{Z}_p} e(ax^2 + bx) |x\rangle dx$$

The following lemma regarding the norm of quadratic Gauss integrals over $p^{-r} \mathbb{Z}_p$ is proven in Lemma 3 in Appendix A.

Lemma 1. Let $\alpha, \beta \in \mathbb{Q}_p$ and $r \in \mathbb{Z}$, then

$$(12) \quad \left| \int_{x \in p^{-r} \mathbb{Z}_p} e(\alpha x^2 + \beta x) dx \right| = \begin{cases} p^{v_p(\alpha)/2} & \text{if } v_p(\alpha) < 2r \text{ and } v_p(\alpha) \leq v_p(\alpha) + r \\ 0 & \text{if } v_p(\beta) < r \text{ and } v_p(\alpha) > v_p(\beta) + r \\ p^r & \text{if } v_p(\alpha) \geq 2r \text{ and } v_p(\beta) \geq r \end{cases}$$

Additionally we define the set $V_\infty^{(r)} \subseteq L^2(\mathbb{Q}_p)$ as

$$(13) \quad V_\infty^{(r)} := \{ |v(\infty, b; r)\rangle : b \in \mathbb{Q}_p \} \text{ with } |v(\infty, b; r)\rangle := p^r \int_{x \in p^r \mathbb{Z}_p} |x - b\rangle dx$$

Note that the $v(\infty, b; r)$ is the Fourier transform of $v(0, b; r)$ and that the V_∞ vectors act like the scaled delta-functions $\sqrt{p^r} \cdot \delta(x - b)$ as $r \rightarrow \infty$.

In Corollary 1 in Appendix A it is proven that for all $a, a' \in \mathbb{Q}_p$ and $b, b' \in \mathbb{Q}_p$ for large enough r we have

$$(14) \quad |\langle v(a', b'; r) | v(a, b; r) \rangle| = \begin{cases} p^{v_p(a-a')/2} & \text{if } a \neq a' \\ 0 & \text{if } a = a' \text{ and } b \neq b' \\ p^r & \text{if } a = a' \text{ and } b = b'. \end{cases}$$

Additionally, with Lemmas 4 and 5 in Appendix A we see that with $a' = \infty$, $a \in \mathbb{Q}_p \cup \{\infty\}$ and $b, b' \in \mathbb{Q}_p$, for large enough r we have the inner product:

$$(15) \quad |\langle v(\infty, b'; r) | v(a, b; r) \rangle| = \begin{cases} 1 & \text{if } a \neq \infty \\ 0 & \text{if } a = \infty \text{ and } b \neq b' \\ p^r & \text{if } a = \infty \text{ and } b = b'. \end{cases}$$

As mentioned before, in the limit $r \rightarrow +\infty$ we have $p^{-r}\mathbb{Z}_p \rightarrow \mathbb{Q}_p$ as sets. Hence with the definitions and results of this section we obtain the main theorem of this article.

Theorem 1. *With the above definitions, all sets $V_\infty^{(\infty)}$ and $V_a^{(\infty)}$ with $a \in \mathbb{Q}_p$ are a basis for $L^2(\mathbb{Q}_p)$. For $a, a' \in \{0, \dots, p-1\}$ it holds that $a - a' = 0$ or $v_p(a - a') = 0$ and hence we have that $\{V_0^{(\infty)}, \dots, V_{p-1}^{(\infty)}, V_\infty^{(\infty)}\}$ makes a set of $p+1$ mutually unbiased bases in $L^2(\mathbb{Q}_p)$ such that for all $a, a' \in \{0, \dots, p-1, \infty\}$ we have the unbiased inner product $|\langle v(a', b'; \infty) | v(a, b; \infty) \rangle| = 1$ when $a \neq a'$.*

In the $r \rightarrow \infty$ limit the functions $v(a, b; r) \in V_a^{(r)}$ are described by

$$(16) \quad V_a^{(\infty)} \ni |v(a, b; \infty)\rangle = \int_{x \in \mathbb{Q}_p} e(ax^2 + bx) |x\rangle dx$$

for all $a, b \in \mathbb{Q}_p$. The elements of $V_\infty^{(\infty)}$ are the Fourier transforms of the $V_0^{(\infty)}$ functions:

$$(17) \quad V_\infty^{(\infty)} \ni |v(\infty, b; \infty)\rangle = \text{Fourier}_{\mathbb{Q}_p} |v(0, b; \infty)\rangle.$$

In Appendix B we have a description of these $(p+1)$ MUBs as eigenfunctions of $(p+1)$ families of unitary transformations on $L^2(\mathbb{Q}_p)$.

4. DIFFERENCE FOR MUBS BETWEEN $L^2(\mathbb{R})$ AND $L^2(\mathbb{Q}_p)$

Why is it that we have $p+1$ MUBs over the p -adic numbers \mathbb{Q}_p , while we only know of 3 MUBs over the reals \mathbb{R} ?

If we want to adapt the $(ax^2 + bx)$ construction to the case of quantum states defined over \mathbb{R} , we can use the normalized Gaussian distribution

$$(18) \quad \frac{\sqrt{2}}{k\sqrt{\pi}} \int_{x=-\infty}^{+\infty} e^{-2(x/k)^2} dx = 1$$

(which in the limit $k \rightarrow +\infty$ gives the ‘uniform distribution over \mathbb{R} ’), to define the basis states

$$(19) \quad |v(a, b; k)\rangle = \sqrt{\frac{\sqrt{2}}{k\sqrt{\pi}}} \int_{x=-\infty}^{+\infty} e^{-(x/k)^2} e^{2\pi i(ax^2+bx)} |x\rangle dx.$$

For the relevant integral we then get

$$(20) \quad \lim_{k \rightarrow +\infty} \left| \frac{\sqrt{2}}{\sqrt{\pi}} \int_{x=-\infty}^{+\infty} e^{2\pi i(\alpha x^2 + \beta x)} e^{-2(x/k)^2} dx \right| \propto \frac{1}{\sqrt{|\alpha|}},$$

which shows that for different bases B_a and $B_{a'}$ we have the dependency

$$(21) \quad |\langle v(a, b; k) | v(a', b'; k) \rangle| \propto \frac{1}{\sqrt{|a - a'|}}.$$

Note now how the norm of the quadratic Gauss integral in Lemma 3 also has a $1/\sqrt{|a|}$ dependency, giving the same kind of dependency of Equation 21. For $L^2(\mathbb{Q}_p)$ however, the $|a|$ is the p -adic norm with $|a| = p^{-v_p(a)}$, which is much more coarse than the standard \mathbb{R} norm. If A is a set of a coefficients, then $\{B_a : a \in A\}$ defines a set of MUBs if $|a - a'| = |a'' - a'''|$ for all $a \neq a', a'' \neq a''' \in A$. For the \mathbb{R} -norm the maximum set A with this property is $A = \{0, 1\}$, while for the p -adic norm we can have $A = \{0, 1, \dots, p-1\}$.

5. CONCLUSION AND OPEN QUESTIONS

We have found that there are at least $p+1$ MUBs if we consider quantum states defined over the p -adic numbers \mathbb{Q}_p , while we only know of 3 MUBs for quantum states defined over the real line \mathbb{R} . An obvious open question is: are these numbers tight, or is it possible to define more MUBs over \mathbb{Q}_p and/or \mathbb{R} ? Upon closer inspection, one can see that the reason why the $(ax^2 + bx)$ construction leads to different MUB situations for \mathbb{Q}_p and \mathbb{R} stems from the fact that their respective norms have different properties. It is another open question if this analysis is only specific to the $(ax^2 + bx)$ construction that we used here, or if this in fact *the* reason why we might have different numbers of MUBs for $L^2(\mathbb{Q}_p)$ and $L^2(\mathbb{R})$.

Acknowledgements. The research presented in this article was supported in part by an NSF CAREER grant (WvD) and by a grant from the Army Research Office (WvD and AR).

REFERENCES

- [1] W.O. Alltop, *Complex sequences with low periodic correlations*, IEEE Transactions on Information Theory, Vol. 26, no. 3, pp. 350–354 (1980).
- [2] Leslie E. Ballentine, *Quantum Mechanics: a modern approach*, World Scientific Publishing, 1998.
- [3] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. 21, Wiley-Interscience, 1998.
- [4] Robin Blume-Kohout, *MUBs in infinite dimensions, the problematic analogy between $L^2(\mathbb{R})$ and \mathbb{C}^d* , Seeking SICs: A Workshop on Quantum Frames and Designs (Waterloo, Ontario, Canada, 2008), available at <http://pirsa.org/08100072/>.

- [5] Nicholas J. Cerf, Mohammed Bourennane, Anders Karlsson, and Nicolas Gisin, *Security of Quantum Key Distribution Using d -Level Systems*, Physical Review Letters, Vol. 88, no. 12, pp. 127902 (2002).
- [6] Cecilia Cormick, Ernesto F. Galvão, Daniel Gottesman, Juan Pablo Paz, and Arthur O. Pittenger, *Classicality in Discrete Wigner Functions*, Physical Review A, Vol. 73, no. 1, pp. 012301 (2006).
- [7] Fernando Q. Gouvêa, *p -adic Numbers: an introduction*, Second Edition, Universitext, Springer, 2000.
- [8] Andreas Klappenecker and Martin Rötteler, *Constructions of Mutually Unbiased Bases*, Finite Fields and Applications, 7th International Conference, Fq7 (2003), Lecture Notes in Computer Science, vol. 2948, Springer, pp. 137–144, available at [arXiv:quant-ph/0309120v1](#).
- [9] S.V. Kozyrev, *Wavelet theory as p -adic spectral analysis*, Izvestiya: Mathematics, Vol. 66, no. 2, pp. 367–376 (2002).
- [10] Dinakar Ramakrishnan and Robert J. Valenza, *Fourier analysis on number fields*, Graduate Texts in Mathematics, vol. 186, Springer, New York, 1999.
- [11] Ph. Ruelle, E. Thiran, D. Verstegen, and J. Weyers, *Quantum mechanics on p -adic fields*, Journal of Mathematical Physics, Vol. 30, no. 12, pp. 2854–2874 (1989).
- [12] V.S. Vladimirov and I.V. Volovich, *p -Adic Quantum Mechanics*, Communications in Mathematical Physics, Vol. 123, pp. 659–676 (1989).
- [13] Stefan Weigert and Michael Wilkinson, *Mutually Unbiased Bases for Continuous Variables*, Physical Review A, Vol. 78, no. 2, pp. 020303(R) (2008), [arXiv:0802.03942v2](#).
- [14] Pawel Wocjan and Thomas Beth, *New Construction of Mutually Unbiased Bases in Square Dimensions*, Quantum Information & Computation, Vol. 5, no. 2, pp. 93–101 (2005), [arXiv:quant-ph/0407081](#).
- [15] William K. Wootters and Brian D. Fields, *Optimal state-determination by mutually unbiased measurements*, Annals of Physics, Vol. 191, no. 2, pp. 363–381 (1989).

APPENDIX A. QUADRATIC GAUSS SUMS AND INTEGRALS

The results in this appendix are not new; see for example Equation 2.11 in [12]. The two main reasons to provide these proofs here is to make the currently article self-contained and to give the reader a flavor of how to do calculations in \mathbb{Q}_p .

A.1. Quadratic Gauss sums over finite rings $\mathbb{Z}/p^k\mathbb{Z}$. The following lemma regarding the norm of quadratic sums over $\mathbb{Z}/p^k\mathbb{Z}$ will be used to prove Lemma 3 about the norm of quadratic Gauss integrals over p -adic numbers.

Lemma 2. *Let $p \neq 2$ be a prime, $k, \ell \in \mathbb{Z}^+$ with $k \geq \ell$, $a, b \in \mathbb{Z}$ and $\omega := e^{2\pi i/p^\ell}$. The quadratic Gauss sum has the following norm*

$$(22) \quad \left| \sum_{x \in \{0, \dots, p^k-1\}} \omega^{ax^2+bx} \right| = \begin{cases} p^{k-\ell/2+v_p(a)/2} & \text{if } a \not\equiv 0 \pmod{p^\ell} \text{ and } v_p(a) \leq v_p(b) \\ 0 & \text{if } b \not\equiv 0 \pmod{p^\ell} \text{ and } v_p(a) > v_p(b) \\ p^k & \text{if } a = b \equiv 0 \pmod{p^\ell}. \end{cases}$$

Proof. Because ω^z is an additive character over $\mathbb{Z}/p^\ell\mathbb{Z}$ we can interpret the values $ax^2 + bx$ modulo p^ℓ . Define and note

$$(23) \quad g(a, b; k, \ell) := \sum_{x \in \{0, \dots, p^k - 1\}} \omega^{ax^2 + bx} = p^{k-\ell} \sum_{x \in \mathbb{Z}/p^\ell\mathbb{Z}} \omega^{ax^2 + bx}$$

$$(24) \quad = p^{k-\ell} \cdot g(a, b; \ell, \ell).$$

To ignore the phase of g , we look at the norm of $gg^* = |g|^2$:

$$(25) \quad |g(a, b; \ell, \ell)|^2 = \left(\sum_{x \in \mathbb{Z}/p^\ell\mathbb{Z}} \omega^{ax^2 + bx} \right) \left(\sum_{y \in \mathbb{Z}/p^\ell\mathbb{Z}} \omega^{-ax^2 - bx} \right)$$

$$(26) \quad = \sum_{x, y \in \mathbb{Z}/p^\ell\mathbb{Z}} \omega^{(x-y)(a(x+y)+b)}$$

Because $p \neq 2$ the mapping $(x', y') = (x - y, x + y)$ can be inverted by $(x, y) = ((x' + y')/2, (y' - x')/2)$, proving that this mapping is a permutation of $(\mathbb{Z}/p^\ell\mathbb{Z})^2$. Hence we can rewrite the summation according to $x \leftarrow (x - y)$ and $y \leftarrow (x + y)$, giving us

$$(27) \quad |g(a, b; \ell, \ell)|^2 = \sum_{x, y \in \mathbb{Z}/p^\ell\mathbb{Z}} \omega^{x(ay+b)}$$

As $\sum_x \omega^{x\delta} = p^\ell$ if $\delta = 0 \pmod{p^\ell}$ and $\sum_x \omega^{x\delta} = 0$ if $\delta \neq 0 \pmod{p^\ell}$ this simplifies to

$$(28) \quad |g(a, b; \ell, \ell)|^2 = p^\ell \cdot |\{y \in \mathbb{Z}/p^\ell\mathbb{Z} : ay + b = 0 \pmod{p^\ell}\}|$$

At this stage we need to calculate how many solutions $y \in \mathbb{Z}/p^\ell\mathbb{Z}$ there are to the linear equation $ay + b = 0 \pmod{p^\ell}$, which depends on the values of a and b modulo p^ℓ . We will have to analyze several cases that can occur depending on whether a or b equal $0 \pmod{p^\ell}$ and the two valuations $v_p(a)$ and $v_p(b)$. If $a \neq 0 \pmod{p^\ell}$, we will write $a = \alpha p^{v_p(a)}$ with $p \nmid \alpha$ and $v_p(a) \in \{0, \dots, \ell - 1\}$. Similarly, if $b \neq 0 \pmod{p^\ell}$, we will write $b = \beta p^{v_p(b)}$ with $p \nmid \beta$ and $v_p(b) \in \{0, \dots, \ell - 1\}$.

- If $a = 0 \pmod{p^\ell}$ and $b = 0 \pmod{p^\ell}$, then there are p^ℓ solutions $y \in \mathbb{Z}/p^\ell\mathbb{Z}$.
- If $a = 0 \pmod{p^\ell}$ and $b \neq 0 \pmod{p^\ell}$, then there are no solutions.
- If $a \neq 0 \pmod{p^\ell}$ and $b = 0 \pmod{p^\ell}$ the equation $\alpha p^{v_p(a)} y = 0 \pmod{p^\ell}$ can be re-expressed as $\alpha y = 0 \pmod{p^{\ell-v_p(a)}}$, which has $p^{v_p(a)}$ solutions $y \in \{0, \dots, p^{v_p(a)} - 1\} p^{\ell-v_p(a)}$.
- If $a, b \neq 0 \pmod{p^\ell}$ and $v_p(a) \leq v_p(b)$, there are $p^{v_p(a)}$ solutions the equation $y = (-\beta/\alpha) p^{v_p(b)-v_p(a)} \pmod{p^{\ell-v_p(a)}}$, namely $y \in (-\beta/\alpha) p^{v_p(b)-v_p(a)} + \{0, \dots, p^{v_p(a)} - 1\} p^{\ell-v_p(a)}$.
- If $a, b \neq 0 \pmod{p^\ell}$ and $v_p(a) > v_p(b)$ there are no solutions to the equation $p^{v_p(a)-v_p(b)} y = (-\beta/\alpha) \pmod{p^{\ell-v_p(b)}}$ as $p \nmid (-\beta/\alpha)$.

Summarizing we have

$$(29) \quad |\{y : ay + b = 0 \pmod{p^\ell}\}| = \begin{cases} p^{v_p(a)} & \text{if } a \neq 0 \pmod{p^\ell} \text{ and } v_p(a) \leq v_p(b) \\ 0 & \text{if } b \neq 0 \pmod{p^\ell} \text{ and } v_p(a) > v_p(b) \\ p^\ell & \text{if } a = b = 0 \pmod{p^\ell}. \end{cases}$$

The combination of Equations 24, 28 and 29 proves the lemma. \square

A.2. Quadratic Gauss integrals over p -adic numbers. With Lemma 2, the following result can be proven.

Lemma 3. *Let $a, b \in \mathbb{Q}_p$ and $r \in \mathbb{Z}$, then*

$$(30) \quad \left| \int_{x \in p^{-r}\mathbb{Z}_p} e(ax^2 + bx) dx \right| = \begin{cases} p^{v_p(a)/2} & \text{if } v_p(a) < 2r \text{ and } v_p(a) \leq v_p(b) + r \\ 0 & \text{if } v_p(b) < r \text{ and } v_p(a) > v_p(b) + r \\ p^r & \text{if } v_p(a) \geq 2r \text{ and } v_p(b) \geq r. \end{cases}$$

Proof. Define and rewrite

$$(31) \quad g(a, b; p^{-r}\mathbb{Z}_p) := \int_{x \in p^{-r}\mathbb{Z}_p} e(ax^2 + bx) dx$$

$$(32) \quad = p^r \int_{x \in \mathbb{Z}_p} e(a(x/p^r)^2 + b(x/p^r)) dx$$

$$(33) \quad = p^r \int_{y \in p^k\mathbb{Z}_p} \sum_{z \in \{0, \dots, p^k-1\}} e(a((y+z)/p^r)^2 + b((y+z)/p^r)) dy$$

$$(34) \quad = p^r \int_{y \in p^k\mathbb{Z}_p} \sum_{z \in \{0, \dots, p^k-1\}} e\left(\frac{a(y^2 + 2yz + z^2) + b(y+z)p^r}{p^{2r}}\right) dy$$

with $k \in \mathbb{Z}^+$. As y is a multiple of p^k , for sufficiently large k (i.e. $k \geq r - v_p(a)/2$, $k \geq 2r - v_p(a)$, $k \geq r - v_p(b)$) the term $(ay^2 + 2ayz + byp^r)/p^{2r}$ can be made an element of \mathbb{Z}_p for all $z \in \mathbb{Z}$, which makes the term irrelevant for the e function. This then gives us the finite summation

$$(35) \quad = p^r \int_{y \in p^k\mathbb{Z}_p} \sum_{z \in \{0, \dots, p^k-1\}} e\left(\frac{az^2 + bzp^r}{p^{2r}}\right) dy$$

$$(36) \quad = p^{r-k} \sum_{z \in \{0, \dots, p^k-1\}} e(ap^{-2r}z^2 + bp^{-r}z)$$

Pick $\ell \in \mathbb{Z}$ such that $\ell \geq 2r - v_p(a)$ and $\ell \geq r - v_p(b)$, making $A = ap^{-2r+\ell}$ and $B = bp^{-r+\ell}$ both elements of \mathbb{Z}_p . We can then rewrite the summation as

$$(37) \quad = p^{r-k} \sum_{z \in \{0, \dots, p^k-1\}} e((Az^2 + Bz)/p^\ell)$$

$$(38) \quad = p^{r-k} \sum_{z \in \{0, \dots, p^k-1\}} e^{2\pi i(Az^2 + Bz)/p^\ell}$$

$$(39) \quad = p^{r-k} \cdot g(A, B; k, \ell).$$

Assume without loss of generality that $k \geq \ell$. Using the previous lemma on Gauss sums over $\{0, \dots, p^k-1\}$ and the fact that $v_p(A) = v_p(a) - 2r + \ell$ and $v_p(B) = v_p(b) - r + \ell$ we get

$$(40) \quad |g(a, b; p^{-r}\mathbb{Z}_p)| = p^{r-k} \cdot |g(A, B; k, \ell)|$$

$$(41) \quad = \begin{cases} p^{v_p(a)/2} & \text{if } v_p(a) < 2r \text{ and } v_p(a) \leq v_p(b) + r \\ 0 & \text{if } v_p(b) < r \text{ and } v_p(a) > v_p(b) + r \\ p^r & \text{if } v_p(a) \geq 2r \text{ and } v_p(b) \geq r. \end{cases}$$

□

Corollary 1. *Let $a, b \in \mathbb{Q}_p$. Define a threshold value $t \in \mathbb{Z} \cup \{-\infty\}$ as follows. If $a = 0$ and $b = 0$ then $t = -\infty$; if $a = 0$ and $b \neq 0$ then $t = v_p(b)$; if $a \neq 0$ then $t = \max\{v_p(a)/2, v_p(a) - v_p(b)\}$. Then, for every $r > t$ we have*

$$(42) \quad |g(a, b; p^{-r}\mathbb{Z}_p)| = \begin{cases} p^{v_p(a)/2} & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \text{ and } b \neq 0 \\ p^r & \text{if } a = b = 0. \end{cases}$$

This last corollary shows that for any $a, b \in \mathbb{Q}_p$ as r gets ‘big enough’, we have the three cases of Equation 42 for the norm of the quadratic Gauss sum. Hence for the case $a \neq 0$ or $b \neq 0$ we have the $r \rightarrow +\infty$ limit

$$(43) \quad \left| \int_{x \in \mathbb{Q}_p} e(ax^2 + bx) dx \right| = |g(a, b; \mathbb{Q}_p)| = \begin{cases} p^{v_p(a)/2} & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \text{ and } b \neq 0. \end{cases}$$

The V_∞ functions of Equation 13 have the same size and orthogonality as the V_a functions as is shown by the following lemma.

Lemma 4. *Use the definitions of Equation 13 and let $b, b' \in \mathbb{Q}_p$. There exists a threshold $t \in \mathbb{Z} \cup \{-\infty\}$ such that for all $r > t$ we have*

$$(44) \quad |\langle v(\infty, b'; r) | v(\infty, b; r) \rangle| = \begin{cases} 0 & \text{if } b \neq b' \\ p^r & \text{if } b = b'. \end{cases}$$

Proof.

$$(45) \quad |\langle v(\infty, b'; r) | v(\infty, b; r) \rangle| = \left| p^{2r} \int_{x, y \in p^r \mathbb{Z}_p} \langle y - b' | x - b \rangle dx dy \right|$$

$$(46) \quad = p^{2r} \mu(\{x \in p^r \mathbb{Z}_p : x + b - b' \in p^r \mathbb{Z}_p\})$$

$$(47) \quad = \begin{cases} 0 & \text{if } v(b - b') < r \\ p^r & \text{if } v(b - b') \geq r \end{cases}$$

Hence we can t be as follows: if $b = b'$, set $t = -\infty$; if $b \neq b'$, set $t = v(b - b')$. \square

The next simple lemma is needed to prove that the V_∞ functions of the main theorem are mutually unbiased to the V_a functions of Equation 11.

Lemma 5. *Let $a, b, c \in \mathbb{Q}_p$. There exists a threshold $t \in \mathbb{Z}$ such that for all $r \geq t$:*

$$(48) \quad \left| p^r \int_{x \in c + p^r \mathbb{Z}_p} e(ax^2 + bx) dx \right| = 1.$$

Proof.

$$(49) \quad \left| p^r \int_{x \in c + p^r \mathbb{Z}_p} e(ax^2 + bx) dx \right| = \left| p^r \int_{x \in p^r \mathbb{Z}_p} e(ac^2 + 2acx + ax^2 + bc + bx) dx \right|$$

For $r \geq \max\{-v_p(2ac + b), -v_p(a)/2\}$ we have that $2acx + ax^2 + bx \in \mathbb{Z}_p$ for all $x \in p^r \mathbb{Z}_p$, which simplifies the integral to

$$(50) \quad = \left| p^r \int_{x \in p^r \mathbb{Z}_p} e(ac^2 + bc) dx \right| = 1.$$

\square

APPENDIX B. A UNITARY DESCRIPTION OF THE $(p+1)$ MUBS IN $L^2(\mathbb{Q}_p)$

As was mentioned in Section 1.2, the three MUBs in $L^2(\mathbb{R})$ can be described as the eigenstates of three Hermitian operators that are combinations of the momentum operator \hat{p} and the position operator \hat{q} . When trying to mimic this approach for the $(p+1)$ MUBs in $L^2(\mathbb{Q}_p)$ one quickly realizes that some complications arise due to the difference between \mathbb{Q}_p and \mathbb{R} . A very concrete example of this complication is the fact that the position operator $\hat{q} : |x\rangle \mapsto x|x\rangle$ does not make sense in this setting as it tries to assign the \mathbb{Q}_p valued position value x as an amplitude. As a way out, we will omit the Hamiltonian description and instead capture the MUBs in terms of the eigenfunctions of $(p+1)$ families of unitary transformations on $L^2(\mathbb{Q}_p)$.

Define the two sets of unitary operators X_c and $Z_d : L^2(\mathbb{Q}_p) \rightarrow L^2(\mathbb{Q}_p)$ with the parameters $c, d \in \mathbb{Q}_p$ by

$$(51) \quad X_c : |y\rangle \mapsto |y+c\rangle \text{ and } Z_d : |y\rangle \mapsto e(yd)|y\rangle \text{ for all } y \in \mathbb{Q}_p.$$

(As $X_c Z_d : |y\rangle \mapsto e(yd)|y+c\rangle$ and $Z_d X_c : |y\rangle \mapsto e(yd+cd)|y+c\rangle$, we have the expected relation $Z_d X_c = e(cd)X_c Z_d$.)

For $a, b, c \in \mathbb{Q}_p$ take $d = 2ac$ and observe that

$$(52) \quad X_c Z_{2ac} : |v(a, b; \infty)\rangle := X_c Z_{2ac} : \int_{x \in \mathbb{Q}_p} e(ax^2 + bx)|x\rangle dx$$

$$(53) \quad \mapsto \int_{x \in \mathbb{Q}_p} e(ax^2 + bx + 2acx)|x+c\rangle dx$$

$$(54) \quad = \int_{x \in \mathbb{Q}_p} e(a(x-c)^2 + b(x-c) + 2ac(x-c))|x\rangle dx$$

$$(55) \quad = e(-bc - ac^2) \int_{x \in \mathbb{Q}_p} e(ax^2 + bx)|x\rangle dx$$

$$(56) \quad = e(-bc - ac^2)|v(a, b; \infty)\rangle,$$

which shows that the $v(a, b; \infty)$ in $V_a^{(\infty)}$ are the eigenfunctions of $X_c Z_{2ac}$ (for all $c \in \mathbb{Q}_p$). Additionally, informally speaking, the (generalized) eigenfunctions of Z_d are those proportional to $|y\rangle$, which are exactly the elements of $V_\infty^{(\infty)}$.

Define the following unitary operator $P_d : L^2(\mathbb{Q}_p) \rightarrow L^2(\mathbb{Q}_p)$ for all $d \in \mathbb{Q}_p$ by

$$(57) \quad P_d : |x\rangle \mapsto e(dx^2)|x\rangle \text{ for all } x \in \mathbb{Q}_p.$$

We immediately have $P_d : |v(a, b; \infty)\rangle \mapsto |v(a+d, b; \infty)\rangle$. We also have, again informally speaking, $\text{Fourier}_{\mathbb{Q}_p} : |v(0, b; \infty)\rangle \mapsto |v(\infty, b; \infty)\rangle$. Hence all $V_a^{(\infty)}$ bases can be obtained through a unitary transformation from the $V_0^{(\infty)}$ basis. As $V_0^{(\infty)} = \{|v(0, b; \infty)\rangle : b \in \mathbb{Q}_p\}$ is exactly the set of characters $x \mapsto e(bx)$ of \mathbb{Q}_p , it is the ‘Fourier basis’ of $L^2(\mathbb{Q}_p)$. By the just described unitary relation between the different bases, we thus have that $V_a^{(\infty)}$ is a basis of $L^2(\mathbb{Q}_p)$ for all $a \in \mathbb{Q}_p \cup \{\infty\}$.

WIM VAN DAM, DEPARTMENT OF COMPUTER SCIENCE, DEPARTMENT OF PHYSICS, UNIVERSITY OF CALIFORNIA, SANTA BARBARA, CALIFORNIA, 93106, UNITED STATES OF AMERICA

ALEXANDER RUSSELL, DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF CONNECTICUT, STORRS, CONNECTICUT, 06269, UNITED STATES OF AMERICA